



DEPARTMENT OF THE NAVY

COMMANDER  
NAVAL RESERVE READINESS COMMAND  
REGION ELEVEN  
1903 DOOLITTLE AVENUE  
FORT WORTH TX 76127-1803

COMNAVRESREDCOMREG11INST 5510.6B

NO1A

COMNAVRESREDCOMREG ELEVEN INSTRUCTION 5510.6B

Subj: CLASSIFIED INFORMATION SECURITY PROGRAM

Ref: (a) SECNAVINST 5510.36  
(b) SECNAVINST 5510.30A

Encl: (1) Emergency Plan

1. Purpose. To publish security procedures for the safeguarding of classified material for REDCOM 11 activities.

2. Cancellation. REDCOMREG11INST 5510.6A. This instruction constitutes a complete revision and should be read in its entirety.

3. Background. Basic to effective security practices is the full understanding that the dissemination of official information requires strict control to prevent sensitive classified information from being used to the detriment of the United States. To this end, classified material control procedures, clearance and access criteria must be adhered to by all members of REDCOM 11. References (a) and (b) are the basic guidance relating to the Security Information Program.

4. Command Management

a. All commanding officers are responsible for effective command management of the information and personnel security program to include:

- (1) Designating a security manager.
- (2) Designating a Top Secret Control Officer if the command handles Top Secret information.
- (3) Designating an Information Systems Security Officer.
- (4) Designating a security officer. (One individual may be both security officer and security manager).
- (5) Preparing written command security procedures.
- (6) Preparing an emergency plan for the protection of classified material.

1394

b. In addition, each command may assign assistant security managers, security assistants and security clerks to assume specific phases of the Information Security Program. These personnel shall be designated by letter.

c. Commands that handle Sensitive Compartmented Information (SCI) have a special security officer designated by Commander, Naval Security Group Command. The SCI program is separate from the Information Security Program and the Command Security Manager does not carry responsibility for it. Cooperation and coordination between the two, especially with regard to investigations and clearances is essential.

d. Duties and responsibilities for the above personnel are contained in reference (a).

5. Security Education. Commanding officers, through their security managers, are responsible for providing security education in their commands. Supervisors are responsible for identifying the security requirements for their work centers and seeing that personnel under their supervision are familiar with the security requirements for their particular assignment. On-the-job training is an essential part of command security education and supervisors should ensure that such training is properly provided and received. Minimum requirements for security education include indoctrination, orientation, on-the-job training, refresher briefings, counterespionage briefings, special briefings, and debriefings. Guidelines for developing a command security education program are contained in reference (a). The senior watch officer at each command, in conjunction with the security manager, will ensure that information and physical security training is incorporated into the qualification standard and training program for all watchstanders. The security manager must be a graduate of the security manager course of instruction or must complete the security manager correspondence course within six months of designation.

6. Personnel Security Clearances. Personnel security clearances shall be processed and recorded per reference (b). All active duty and Selected Reserve personnel will have, at a minimum, a valid ENTNAC or NAC investigation. Personnel requiring continued access to Top Secret information must undergo a periodic reinvestigation every five years.

7. Classified Information Non-Disclosure Agreements (NDA) and Security Termination Statements

a. Per reference (a) and Executive Order 12356, all Department of the Navy (DON) personnel holding security

clearances are required to have a signed SF 189, SF 189-A, or the new SF 312 Non-Disclosure Agreement (NDA) on file with the Naval Investigative Service Command (Code 29) and a copy in their service record.

b. Refusal to execute a SF 312 or absence of a SF 189 or SF 189-A executed by DON personnel will be grounds for denial of access to classified information.

c. The debriefing acknowledgment portion of SF 312 will not be used in the DON. Use the Security Termination Statement (OPNAV 5511/14) instead.

d. Debriefings will be conducted under the conditions set forth in reference (a). Personnel being debriefed will execute a Security Termination Statement (OPNAV 5511/14).

8. Routing, Control, and Destruction of Classified Material  
Commands will establish routing, control and destruction procedures for classified material using methods described in reference (a).

9. Storage and Security

a. Minimum stowage requirements set forth in reference (a) shall be set by all commands.

b. Care of classified material during working hours:

(1) When classified documents are removed from storage for working purposes, they are to be kept face down or covered when not actually in use.

(2) Visitors will be controlled to preclude access to classified material.

(3) Classified material will not be discussed over non-secure telephones.

(4) Classified material will not be telefaxed.

(5) Preliminary drafts, carbon sheets, etc., will be destroyed as directed by reference (a) or will be given the appropriate classification and safeguarded in the same manner as the classified matter resulting from them.

(6) Classified information will not be entered into data processing equipment unless the equipment is properly protected and certified for classified use.

17 JUL 1990

(7) Registered mail will be treated as secret material until the security classification is determined.

c. Care of classified material after working hours.

(1) All classified material will be stowed per reference a). Under no circumstances will classified material be stored with money, paychecks, or highly pilferable items.

(2) In securing safes containing classified material, combination lock dials shall be turned at least four complete times in each direction and all drawers or doors shall be tested in the locked position.

(3) A Security Container Check Sheet (SF 732) shall be attached to each cla

(7) Registered mail will be treated as secret material until the security classification is determined.

c. Care of classified material after working hours:

(1) All classified material will be stowed per reference (ssified security container and initialed upon opening and closing the container.

(4) Prior to securing, custodians will ensure that no classified material is adrift and safes are secured.

d. In the event of a fire or other emergency, classified material will be stowed in the same manner as at the end of the day.

e. Open safe. Any member finding a classified material container open in the absence of assigned personnel shall immediately post a guard and notify the duty watchstander and person(s) responsible for the contents of the container. The individual responsible for the contents of the container shall conduct an inventory to determine if the material has been compromised. If the possibility of a compromise exists, it shall be reported using the procedures outlined in reference (a).

f. Recording and changing of safe combinations.

(1) All safes containing classified material shall have their combinations recorded on a Security Container Information Card (SF 700) and stored in the commanding officer's or security manager's safe.

(2) Combinations will be changed when required under the conditions listed in reference (a).

*Ed J. ...*

g. All security containers will have the following:

(1) Security Container Check Sheet (SF 702).

(2) A completed Security Container Information Card (SF 700) Part I, attached to the inside of each safe.

10. Reproduction or Removal of Classified Material. Classified material shall not be reproduced or removed from the physical confines of any activity without the knowledge and approval of the security manager. Reprographic equipment must clearly indicate the highest classification of material which may be copied. Personal copiers may not be brought aboard REDCOM 11 activities. Personal cameras may not be introduced into any space where classified material is handled or stored.

11. Forms. All forms listed in this instruction may be obtained through the supply system.

12. OPSEC

a. The primary goal when planning, preparing for, and executing military operations and other activities is to accomplish the assigned mission. When mission accomplishment and effectiveness are relative to what others can and cannot do, advantages can be gained and harm avoided by essential secrecy about intentions, capabilities, and current activities.

b. OPSEC is the process of planning and action associated with operations and other activities to protect essential secrecy. The aim of OPSEC is to neutralize the threat of foreign information gathering and synthesis capabilities that support hostile planning and decision making.

c. To ensure that Reservists are provided basic OPSEC concepts, OPSEC orientation will be included during initial training and annually.

*J. N. H. Costas*

J. N. H. COSTAS

Distribution: (REDCOMREG11INST 5216.1P)

List A

B-2 (w/o encl)

4 8 JUL 68

NAVAL RESERVE READINESS COMMAND REGION ELEVEN  
EMERGENCY PLAN

1. Purpose. The purpose of the emergency action plan is to protect and minimize the risk of compromise of the command's classified holdings during crisis or emergency situations.

2. Emergency Action

a. Types of Threats

(1) Natural Disaster. In the event of a natural disaster threatening the integrity of the building, responsible personnel will ensure all classified material is secured in proper containers.

(2) Civil Disturbance. In the event of a civil disturbance of such magnitude as to risk compromise of classified material, responsible personnel shall ensure all classified material is secured in proper containers. Emergency destruction will be implemented only when deemed necessary by competent authority.

b. Emergency Destruction. Emergency destruction procedures will be implemented only at the direction of the Security Manager, Chief of Staff or Deputy, Readiness Commander, as circumstances dictate.

3. STU-III Planning Procedures. For matters of STU-III keying material, this command is a subcustodian of Naval Air Station, Joint Reserve Base, Fort Worth. Guidance concerning emergency disposition or destruction of STU-III materials shall be obtained from the primary custodian.

Encl (1)